

CO WIEDZĄ O TOBIE INNI? ILUZJA ANONIMOWOŚCI W INTERNECIE

Kamil Ruszkowski
Uniwersytet Mikołaja Kopernika w Toruniu
Wydział Matematyki i Informatyki
ruszkowskik@mat.umk.pl

Abstract. *This work discusses the common misconceptions regarding the perception of anonymity. It deconstructs the myth of an IP address being a primary user identifier and presents the factual level of risk connected to it. The paper also discusses that VPNs and proxies are not essential in protecting privacy and describes the role of digital footprint as an actual identification factor. It introduces good habits that help users preserve their anonymity and suggests blockchain as a valuable addition to their privacy-related portfolio.*

1. Wstęp

Szybki rozwój technologii drastycznie zmienił sposób, w jaki dziś społeczeństwo rozumie interakcje społeczne, konsumpcję dóbr i wiele innych, ważnych aspektów codziennego życia, a co za tym idzie, zaczęła również rosnąć ilość wiedzy, którą ktoś musi posiadać, aby mieć aktualne i zgodne z prawdą informacje na temat tych zmian. Przykrym faktem jest to, że znacząca większość społeczeństwa czerpie wiedzę na tematy naukowe i technologiczne z telewizji i social mediów, a tylko mniej niż 10% sięga po specjalistyczne czasopisma [6].

Głównymi zagrożeniami wynikającymi z takiego sposobu doboru źródeł są: niezrozumienie otaczającego nas świata oraz przydatności nauki w życiu codziennym [7], podatność na manipulację i tzw. postprawdę [23] (promowaną przez polityków, przykładem może być, chociażby sprawa ujawnienia danych osobowych „hejtera” przez wiceministra Gramatykę i rozpoczęcie dyskusji o zmniejszeniu anonimowości, w oparciu głównie o emocje [19]) oraz wyjaśnianie zachodzących zjawisk nienaukowymi metodami (np. przekonaniem osoby o tym, jak jakiś element powinien logicznie działać).

Z powodu stronniczego podejścia mediów do tematu anonimowości w Internecie [22] oraz braku edukacji w temacie schematów działania komunikacji w Internecie, mamy do czynienia z ogromem mitów np. na temat identyfikacji użytkowników po samym adresie IP, lub tym, że „nikt w Internecie nie jest anonimowy”, niezależnie od kontekstu sytuacji i jego aktywności w sieci, gdzie w praktyce, nawet oszuści są poza

zasięgiem służb ze względu na braki w kadrach i zasobach [5]. Użytkownicy, pomimo wiedzy o skutkach podawania przez nich danych osobowych w sieci, nie czytają polityk prywatności i nie wskazują jako składowych swojego digital footprintu elementów takich jak przeglądarka, system operacyjny oraz cookies, nie uważają również za konieczne chronienie takich danych, jak historia przeglądania, zachowania w sieci oraz imię, nazwisko, narodowość, itd. [3]

2. Mit adresu IP jako głównego identyfikatora

Duża część użytkowników postrzega wyciek adresu IP jako spore zagrożenie dla ich prywatności, gdy w rzeczywistości pozwala on tylko (ale w przypadku służb nie tylko, mogą oni bowiem uzyskać od dostawcy Internetu pełne dane abonenta) na określenie przybliżonej lokalizacji geograficznej oraz ujrzenie bardzo ograniczonego zakresu aktywności użytkownika w sieci [28]. Dzieje się tak, ponieważ NAT (Network Address Translation) pozwala na ukrycie całej sieci wewnętrznej złożonej z wielu urządzeń pod jednym adresem IP. Chroni to sieć przed dostępem z zewnątrz oraz rozróżnieniem pojedynczych maszyn po samym adresie IP [12]. Problemem w używaniu NAT może być podatność na ataki, wynikająca ze złej konfiguracji oraz luk w ALG (Application Level Gateway, pozwala na usprawnienie komunikacji przez NAT poprzez dodanie dodatkowych reguł zarządzania połączeniami i przekazywania informacji) [15]. Mówiąc o temacie ukrywania adresu IP przed innymi, nie sposób przejść obojętnie wobec VPNów i proxy. Pierwsze z nich są dużo bardziej utrwalone w świadomości konsumentów, jako dobry i prosty sposób na zupełną anonimowość i tak też są reklamowane.

W czasach sprzedawania danych użytkowników przez coraz więcej podmiotów, w opinii publicznej lepiej jest korzystać z usług dostawców VPN, niż pozwalać swojemu dostawcy wykorzystywać nasze dane, ale w praktyce jest to po prostu przenoszenie zaufania z jednego źródła do drugiego [26]. Warto nadmienić, że weryfikowalność transparentności i uczciwości obu tych źródeł jest taka sama, czyli znikoma; nawet jeśli same organizacje nie sprzedają danych, nie mamy pojęcia, czy właściciele serwerów, lub podmioty trzecie tego nie robią.

Kolejnym zagrożeniem związanym ze zdecydowaniem się na VPN jest ryzyko luk w zabezpieczeniach po stronie dostawców tychże usług [21, 27]. Brak możliwości zbadania wiarygodności zapewnień o polityce no-log oraz wcześniej wspomniane luki i podatności skutkują ryzykiem deanonimizacji użytkownika, który przez cały ten czas ma poczucie pełnej prywatności.

Ważnym argumentem stojącym w kontrze do skuteczności VPNów jest tzw. digital footprint, dzięki któremu serwisy i tak rozróżnią użytkownika, nawet pomimo zmiany adresu IP. Dokładniejsze wyjaśnienie działania cyfrowego śladu znajduje się w dalszej części pracy. Kolejnym, mniej popularnym, rozwiązaniem stosowanym w celu ukrycia swojego IP są serwery proxy. Polegają one na przekierowywaniu zapytań klienta przez pośrednika (proxy), w celu zachowania anonimowości. W Internecie dostępnych jest

dużo darmowych proxy, jednak większość z nich albo nie spełnia swojej funkcji (ujawnia IP klienta), albo, w przypadku niedostatecznie zabezpieczonej komunikacji, manipuluje ruchem, wstrzykując złośliwe oprogramowanie w postaci trojanów, skryptów, bądź próbuje wykorzystać klienta w celu wydobywania kryptowalut [1].

Płatne serwery proxy z kolei, podobnie jak VPNy, są podatne na gromadzenie informacji o aktywności użytkownika i dalsze ich przetwarzanie. Problemem obu rodzajów serwerów proxy jest także wysoki procent ich blacklistowania [20], co uniemożliwia wygodne korzystanie z Internetu i przeczy celowi używania takich rozwiązań.

3. Rola digital footprintu w pozyskiwaniu danych o użytkowniku

Wiedząc już, że adres IP nie pozwala na uzyskanie zbyt wielu informacji warto przyjąć się digital footprintowi. Jest to zestaw aktywności, cech i danych, które umożliwiają rozpoznanie unikatowego użytkownika w Internecie. Zestaw ten jest znacznie większy, niż można przypuszczać; składa się bowiem z takich elementów jak system operacyjny, strefa czasowa, język, cookies, wersja przeglądarki, ale także hardware, czy aktywność w sieci [2][3]. Warto w tym miejscu skupić się na cookies, gdyż jest to element, którego działanie nie jest rozumiane przez większość społeczeństwa [24].

Cookies dzielą się na dwa typy. Pierwszym z nich są session cookies, czyli takie, które wygasają po zamknięciu sesji i służą np. do zapamiętywania zawartości koszyka w sklepie internetowym. Drugim typem są permanent cookies, czyli takie, które zapisywane są na urządzeniu i służą identyfikacji Internauty od razu po uruchomieniu strony [24]. Znacząca większość ciasteczek nie jest wymagana do poprawnego działania strony; ogromny procent stanowią te wykorzystywane do celów marketingowych [24]. Należy nadmienić, że istnieją przeglądarki i rozwiązania, które domyślnie usuwają cookies, na które zgodził się użytkownik (np. Firefox Focus), aczkolwiek popularne przeglądarki również obsługują taką funkcjonalność w postaci wtyczek, lub odpowiednich pól w ustawieniach [16]. W takich realiach poszukiwanie rozwiązania, które zapewni użytkownikowi większą prywatność i anonimowość staje się dużo cięższe, niż opłacenie dostawcy VPN, lub dostępu do serwera proxy.

Cyfrowy ślad zostawia również dużo większe pole do przetwarzania danych już zidentyfikowanego użytkownika. Przykładem tego jest chociażby afera związana z Cambridge Analytica, organizacją, która bez wiedzy użytkowników zbierała ich dane z Facebooka, aby je przetwarzać i lepiej dopasowywać politycznie nacechowane reklamy [9]. Sprawa ta jest powszechnie uznawana za bezpośrednią ingerencję w demokrację; jest również jednym z największych pod względem skali przypadków wykorzystania elementów cyfrowego śladu [9]. Dane takie jak system operacyjny, czy internetowe nawyki mogą także pomóc podmiotom zewnętrznym odróżniać użytkowników ukrywających się

za NATem, na przykład poszczególnych domowników, aby lepiej dopasowywać proponowane im reklamy.

Większym zagrożeniem dla anonimowości użytkowników jest jednak możliwość wykorzystania ich danych przez innych Internautów. Rozwój białego wywiadu (Open-Source Intelligence / OSINT) pozwolił na ustalanie dokładnego miejsca zamieszkania, danych osobowych, terminów wyjazdów i wielu innych, bardzo prywatnych informacji praktycznie każdemu, kto posiada wystarczająco dużo wytrwałości. O ile samo ustalenie takich danych nie stanowi jeszcze bardzo dużego zagrożenia (oczywiście jeśli osoba, która je ustaliła nie robiła tego z intencją zrobienia komuś krzywdy), tak ich publikacja wystawia ofiarę na spore ryzyko. Zjawisko to nazywa się doxingiem i jest bardzo często spotykane w Internecie w różnych formach; niektóre takie działania są podejmowane w ramach samosądu, bądź też pomocy policji w złapaniu sprawcy. Przykładem takiej sytuacji jest reakcja użytkowników 4chana, którzy w odpowiedzi na znęcanie się nad zwierzętami, podali w Internecie pełne dane, adresy, numery telefonów i wizerunki obu sprawczyń, a także zawiadomili lokalną prasę i organy ścigania [11]. Jednak nie zawsze wymagane jest sprowokowane Internautów niemoralnymi działaniami; czasem wystarczy specyficzne poczucie humoru i chęć trollowania bez większego celu. Świadczy o tym chociażby sytuacja amerykańskiego performerera, Shia LaBeoufa, którego wystawy poświęcone sprzeciwowi wobec prezydentury Donalda Trumpa padały kolejno ofiarą użytkowników 4chana, którzy to wysledzili dokładną lokalizację jednej z takich transmisji po ułożeniu gwiazd na niebie, smug po lotach samolotów oraz zdjęciach fanów z Shią, którzy opublikowali je w zbliżonym do rozpoczęcia transmisji czasie [13].

Dowiedziawszy się, jakie konsekwencje może mieć analiza naszego cyfrowego śladu przez osoby niepowołane oraz jaką może mieć on skalę, warto sprawdzić, jakie dane ktoś może znaleźć na nasz temat przy względnie niedużych nakładach pracy. Można zacząć od odwiedzenia trzech następujących stron:

- <https://amiunique.org/> - wyświetla informacje o cyfrowym odcisku użytkownika. Wskazuje na wagę różnych czynników w identyfikacji (np. języka, strefy czasowej, rozmiaru ekranu, czy czcionek).
- <https://pimeyes.com/en> – po wczytaniu wskazanego zdjęcia wyszukuje wszystkie zdjęcia tej samej osoby w Internecie. Dzięki temu narzędziu można zobaczyć swój wizerunek publikowany w nieoczywistych miejscach (korzystając z tego narzędzia, znalazłem zdjęcie siebie w tłumie opublikowane 8 lat temu przez lokalny dziennik).
- <https://web.archive.org/> - internetowe archiwum, w którym znajduje się bardzo wiele informacji, nawet tych usuniętych dawno temu. Skasowane wpisy, konta w mediach społecznościowych, blogi i zdjęcia; jest spora szansa, że waybackmachine pozwoli każdemu Internaucie uzyskać ponowny dostęp do tych danych.

Dzięki nim możliwe jest sprawdzenie w jakim stopniu jesteśmy identyfikowalni, co pozwala na wyrobienie lepszych nawyków i zastanowienie się, czy na pewno wystarczająco bezpiecznie zarządzamy swoim cyfrowym wizerunkiem.

4. Blockchain a anonimowość

Stosunkowo rzadko poruszany medialnie tematem w kontekście anonimowości jest blockchain. Jest to jednokierunkowa lista wpisów (bloków), składających się z timestampa, danych transakcji oraz haszu poprzedniego elementu. Można ją przedstawić w postaci łańcucha bloków, gdzie każdy blok symbolizuje jedną transakcję. Łańcuch ten jest nierozzerwalny (próba zmiany któregoś z bloków tworzy fork, który jest niezależny od pierwotnego łańcucha), niezmienny i publiczny, czyli każda strona mająca dostęp widzi go w tej samej postaci, a transakcji dokonanych nie można już cofnąć [8]. Kolejną cechą blockchaina jest pseudonimowość (w przypadku np., Bitcoina, lub Ethereum), bądź anonimowość (przykładem jest Monero lub Zcash) [25]. Dzięki bardzo silnym algorytmom kryptograficznym blockchain stanowi dobry sposób na bezpieczne przechowywanie wrażliwych danych, takich jak hasła, dane medyczne, czy istotne dokumenty [4]. Taki sposób organizacji informacji zmniejsza ryzyko wycieków, a więc wzmacnia prywatność. Warto również nadmienić, że pseudonimowe transakcje (czyli te dokonywane np. za pomocą Bitcoina) można śledzić, a gdy użytkownik postanowi podać adres swojego portfela, bądź wypłacić pseudonimową walutę bez wcześniejszego miksowania i dywersyfikowania [29] jej, to cały łańcuch staje się jawny i traci jakiegokolwiek cechy anonimowości.

Znając adres portfela Ethereum, bądź Bitcoina bardzo łatwo można skorzystać ze stron poświęconych rejestrowaniu transakcji blockchain i na żywo monitorować cały przepływ środków [10]. Metody te wykorzystuje na przykład twórca internetowy Coffeezilla podczas ujawniania oszustw i manipulacji innych twórców i celebrytów [14]. Część giełd wymaga również potwierdzenia swojej tożsamości przed obrotem kryptowalutami, co również może utrudniać zachowanie pełnej prywatności przepływu środków. Kolejnym utrudnieniem, również związanym z pseudonimowymi walutami, są legislacje i obstrzeżenia dotyczące istnienia niektórych mikserów. Służą one przeciwdziałaniu praniu brudnych pieniędzy, ale niestety konsekwencje w postaci zwiększonej transparentności transakcji dotyczą również uczciwych użytkowników [18].

5. Jak zwiększyć swoją prywatność? Praktyczne wskazówki

Temat anonimowości w Internecie jest bardzo rozległy i nie sposób w jednym tekście omówić wszystkich niuansów, zagrożeń i zasad bezpieczeństwa. Dlatego też praca skupia się głównie na roli cyfrowego śladu w identyfikacji użytkowników i omawia mit IP jako identyfikatora i źródła zagrożeń prywatności. W nawiązaniu do tego, warto wdrożyć do codziennej rutyny następujące czynności:

- Korzystanie z kilku adresów email – korzystanie ze wszystkich social mediów zarejestrowanych przy użyciu jednego adresu email to łatwy sposób na połączenie danych i zebranie większej ilości informacji o użytkowniku przez stronę trzecią
- Unikanie oversharingu – przed umieszczeniem jakiegokolwiek wpisu, bądź zdjęcia na social mediach należy zastanowić się dwa razy – w Internecie nic nie ginie
- Wykorzystanie technologii blockchain – zwiększone bezpieczeństwo przechowywanych danych, szczególnie tych wrażliwych, to dobry dodatek do reszty bardziej popularnych rozwiązań. Jeśli nie dojdzie do wycieku informacji, nikt nie zostanie zdeanonimizowany. Jeśli natomiast chodzi o transakcje, to dobrze jest skorzystać z kryptowalut zapewniających anonimowość i przestrzegać ich procedur bezpieczeństwa
- Sprawdzanie swojego digital footprintu – ktoś mógł bez zgody umieścić zdjęcie z naszym wizerunkiem, mogło dojść do wycieku danych; regularne sprawdzenie, czy nasza podaż danych nie jest zbyt duża to dobry nawyk
- Korzystanie z technologii wspomagających anonimowość – zainstalowanie Tails, Whonix, czy Tor Browser pomoże zmniejszyć cyfrowy ślad. Oczywiście jeśli nie będziemy logowali się na konta, które pozwolą nas zidentyfikować i zmienimy nawyki dotyczące podaży informacji w sieci
- Uważne czytanie polityk prywatności, użycia danych i odpowiedzialne włączanie cookies – w większości przypadków nie powinniśmy odruchowo klikać „Zgoda”. Chwila poświęcona na zapoznanie się z konsekwencjami naszego kliknięcia pozwoli na przykład na zminimalizowanie przekazywania naszych danych podmiotom zewnętrznym.

Literatura

1. A. Mani, T. Vaidya, D. Dworcen, and M. Sherr, “An extensive evaluation of the internet’s open proxies,” *Proceedings of the 34th Annual Computer Security Applications Conference*, pp. 252–265, Dec. 2018. doi:10.1145/3274694.3274711
2. A. Salomatin, A. Iskhakov, and R. Meshcheryakov, “Formation of a digital footprint based on the characteristics of computer hardware to identify apcs users,” *2021 International Russian Automation Conference (RusAutoCon)*, pp. 314–320, Sep. 2021. doi:10.1109/rusautocon52004.2021.9537361
3. A. Tozzi and G. Coppola, “Digital Footprint Awareness,” <https://www.dlearn.eu/>, <http://dlearn.eu/wp-content/uploads/2020/02/Report-Digital-Footprint-Awareness-2020.pdf>.
4. B. Ram and P. Verma, “Application of blockchain technology in Data Security,” *IP Indian Journal of Library Science and Information Technology*, vol. 9, no. 1, pp. 51–55, Aug. 2024. doi:10.18231/j.ijlsit.2024.008

5. D. Michalecki, "Przestępstwa internetowe: zapobieganie i zwalczanie – obywatele bez ochrony," *Najwyższa Izba Kontroli*, vol. 5, 2023.
6. Directorate-General for Research and Innovation (European Commission), "European citizens' knowledge and attitudes towards science and technology," *Eurobarometer Report*, pp. 51–55, Feb. 2025. .
7. Directorate-General for Research and Innovation (European Commission), "European citizens' knowledge and attitudes towards science and technology," *Eurobarometer Report*, pp. 65–68, Feb. 2025.
8. F. J. de Haro-Olmo, Á. J. Varela-Vaca, and J. A. Álvarez-Bermejo, "Blockchain from the perspective of privacy and Anonymisation: A systematic literature review," *Sensors*, vol. 20, no. 24, Dec. 2020. doi:10.3390/s20247171
9. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal
10. <https://www.blockchain.com/explorer>
11. <https://www.dailydot.com/unclick/florida-girls-kill-rare-tortoise/>
12. <https://www.ibm.com/docs/en/i/7.4.0?topic=translation-masquerade-hide-nat>
13. <https://www.netwatchglobal.com/solutions/capture-the-flag-using-osint-techniques/>
14. <https://www.newyorker.com/news/letter-from-the-southwest/coffeezilla-the-youtuber-exposing-crypto-scams>
15. <https://www.securityweek.com/nat-slipstreaming-visiting-malicious-site-can-expose-local-network-services-remote-attacks>
16. <https://support.mozilla.org/en-US/kb/block-cookies-firefox-focus-android>
17. <https://support.torproject.org/glossary/cookie/>
18. <https://www.theverge.com/2022/8/8/23296778/us-treasury-tornado-cash-crypto-mixer-sanctions-ethereum-north-korea>
19. <https://wiadomosci.gazeta.pl/wiadomosci/7,114884,31677684,wiceminister-opublikowal-dane-internauty-w-koalicji-zawrzalo.html>
20. J. Choi *et al.*, "Understanding the proxy ecosystem: A comparative analysis of residential and open proxies on the internet," *IEEE Access*, vol. 8, pp. 111368–111380, 2020. doi:10.1109/access.2020.3000959
21. K. Qollakaj and L. E. Larsson, "Cybersecurity of remote work migration: A study on the VPN security landscape post covid-19 outbreak," <https://www.diva-portal.org/smash/get/diva2:1778036/FULLTEXT03.pdf>.
22. K. Trytko, "Blessing or curse of the digital world — perceptions of online anonymity in Polish daily newspapers," in *Central European Journal of Communication*, pp. 247–261, vol. 2, 2015.
23. Ł. Danel, "Rozdział I. Rozumienie „post-prawdy”," in *Post-prawda : jak rodzą się społeczne bzdury? Raport*, Kraków: Małopolska Szkoła Administracji Publicznej Uniwersytetu Ekonomicznego, 2022

24. M. A. Shehu, S. E. Song, and E. J. Avong, "Security and Privacy Concern of Web Cookies, with User's Understanding and Management of their Web Cookie," *International Journal of Computer Science and Network*, vol. 9, no. 3, pp. 130–139, Jun. 2020.
25. N. Alsalami and B. Zhang, "SOK: A systematic study of anonymity in cryptocurrencies," *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 1–9, Nov. 2019. doi:10.1109/dsc47296.2019.8937681
26. R. Ramesh, A. Vyas, and R. Ensafi, "All of them claim to be the best': Multi-perspective study of VPN users and VPN providers," https://www.researchgate.net/publication/362567899_All_of_them_claim_to_be_the_best_Multi-perspective_study_of_VPN_users_and_VPN_providers, https://www.researchgate.net/publication/362567899_All_of_them_claim_to_be_the_best_Multi-perspective_study_of_VPN_users_and_VPN_providers.
27. T. Rytilahti and T. Holz, Bad neighbors: On understanding VPN provider networks, https://www.researchgate.net/publication/384887061_Bad_Neighbors_On_Understanding_VPN_Provider_Networks.
28. Technology Analysis Branch of the Office Privacy Commissioner of Canada, "What an IP address can reveal about you," https://www.priv.gc.ca/media/1767/ip_201305_e.pdf.
29. U. W. Chohan, "The cryptocurrency tumblers: Risks, Legality and Oversight," *SSRN Electronic Journal*, Nov. 2017. doi:10.2139/ssrn.3080361